User's Guide

PowerAlert® Element Manager

WARRANTY REGISTRATION

Register your product today and be automatically entered to win an ISOBAR® surge protector in our monthly drawing!

tripplite.com/warranty

Table of Contents

1. Introduction

The PowerAlert Element Manager (PAEM) is a software application that facilitates configuration and maintenance of Tripp Lite LX Platform devices. PAEM contains a discovery engine to identify supported Tripp Lite solutions on the network. PAEM then leverages this information when performing the following functions:

• **Mass Configuration** – Concurrently applying a source configuration to multiple target devices.

• **Mass Update** – Concurrently installing LX Platform firmware onto multiple LX Platform devices.

1.1 Supported Platforms

PAEM operates with the following software and hardware platforms:

• LX Platform Hardware:

  • WEBCARDLX, WEBCARDLXMINI

  • Slotted UPS systems (e.g. SMART750RM1U)

  • UPS systems with preinstalled WEBCARDLX (e.g. SMART750RM1UN)

  • Monitored LX PDUs (e.g. PDU3EVN series)

  • Switched LX PDUs (e.g. PDU3EVSR series)

  • PDUs with preinstalled WEBCARDLX (e.g. PDUMNH20)

  • Slotted ATS systems (e.g. PDUMH15AT)

  • ATS systems with preinstalled WEBCARDLX (e.g. PDUMH15ATNET)

  • SRCOOLNETLX, SRCOOLNET2LX

  • Slotted SRCOOL models e.g. SRCOOL18K

PAEM does NOT operate with the following platforms:

• SNMPWEBCARD Platform (e.g. legacy PDUs, SRCOOLNET, etc.)

• PowerAlert Local Software (PAL)

• PowerAlert Network Management System Software (PANMS)

• PowerAlert Network Shutdown Agent Software (PANSA)

• Tripp Lite KVMs

• Tripp Lite Managed Switches

• Tripp Lite Console Servers

• Non-Tripp Lite devices

1. Introduction

1.2 Supported Mass Configurations

PAEM supports the following mass configurations:

• Between identical LX Platform device models (e.g. PDU15NETLX to PDU15NETLX)

• Between LX devices of the same product family (e.g. PDUMNV15 to PDUMNV30)

• Between LX device model types (e.g. a monitored PDU to one or more switched PDUs)

• Between device types within the LX Platform (e.g. a PDU to one or more UPS systems)

• Within firmware platforms (i.e. version 15.5.x to 15.5.x and 20.x.x to 20.x.x)

• Across firmware platforms (i.e. version 15.5.x to 20.x.x and 20.x.x to 15.5.x)

Note that during mass configurations between firmware platforms, dissimilar configuration parameters will be disregarded. For example, firmware version 15.5.x supports Realms, whereas version 20.x.x does not. Conversely, firmware version 20.x.x supports Privileges, whereas 15.5.x does not. During a mass configuration from 15.5.x to 20.x.x, any Realm configurations will be disregarded—PAEM will not "translate" Realms to equivalent Privileges. This also applies to log settings; due to log differences between 15.5.x and 20.x.x, log settings must be manually edited after the upgrade or downgrade.

Similarly, mass configurations between different device types (e.g. PDU to UPS) will ignore dissimilar or unique parameters:

Shared Parameters

• Local Users

• Network Services

• SMTP Settings

• AAA Settings

• Security Servers

• Syslog Servers

• Time Settings

• Auto Probes

• SNMP Alert Contacts

• SMTP Alert Contacts

• SMS Alert Contacts

• SNMPv1, v2 Users

• SNMPv3 Users

• Accounting Log

• Data Log

• Application Log

• Event Log

• Default Display Settings

• Password Settings

• Roles

Ignored Parameters

• Devices

• Actions

• Loads

• load groups

• Events

• Variables

• Schedules

1. Introduction

1.3 Supported Firmware Updates and Downgrades

PAEM supports the following firmware updates:

• Maintenance releases within a platform, for instance from 15.5.1 to 15.5.3

• Minor releases within a platform, for instance from 20.0.x to 20.1.x

• Major releases for instance from 15.5.x to 20.0.x

• Devices must be running firmware version of 15.5.2 or higher in order to upgrade to PADM20 (if devices are running firmware versions 15.5.1 or earlier, they must be upgraded to 15.5.7 prior to the PADM20 upgrade)

PAEM supports the following firmware downgrades:

• Maintenance releases within a platform, for instance from 15.5.3 to 15.5.1

• Minor releases within a platform, for instance from 20.1.x to 20.0.x

• Major releases, down two increments, for instance from 20.1.x to 15.5.7

Notes:

• *PAEM does NOT support updates or downgrades of firmware versions earlier than 15.5.1.*

• *The only supported major release downgrade is to 15.5.7. If a downgrade is needed to an earlier version, first perform the major release downgrade to 15.5.7, then a maintenance release downgrade to the desired version.*

• *A major release downgrade to 15.5.7 will reset the LX interface to Factory Default Settings and will not retain network settings; it will revert to DHCP.*

1.4 System Requirements

• Personal computer with a supported operating system: Windows 7, 8 or 10; Windows Server 2008, 2012, 2016 or 2019

• CPU: 4 core 2.0 GHz or higher

• Memory: minimum of 1.5 GB

• Disk Space: minimum of 40 GB

• Ethernet network that supports the TCP/IP protocol

• Supported web browser: Google Chrome, Mozilla Firefox, Internet Explorer 10 or later, Safari

PAEM operations may fail when executed remotely. Ensure that the network administrator lifts network restriction that block outgoing HTTP/HTTPS traffic from the device to the PAEM HTTP/HTTPS Port.

Download the latest version of PowerAlert Element Manager from the Tripp Lite website at tripplite.com/products/management-software

For detailed instructions on installing PAEM, refer to the PAEM Installation Guide.

2. Launching PAEM

2.1 Local Access

During PAEM installation, a PAEM icon (Figure 2-1) is added to the desktop of the computer. To access PAEM from this computer, double-click the icon.

Figure 2-1: PAEM Desktop Icon

2.2 Remote Access

To access PAEM remotely, open a supported web browser. In the address bar, enter the IP address of the server on which PAEM is installed, followed by the configured port, e.g. http://192.168.1.1:8080 (Figure 2-2).
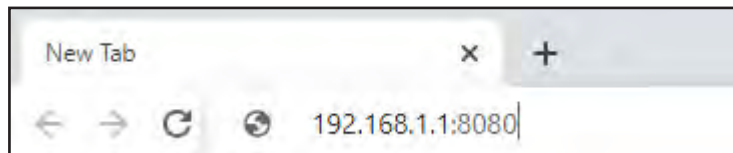

Figure 2-2: Accessing PAEM from a Web Browser

The default Login and Password are both **localadmin**.
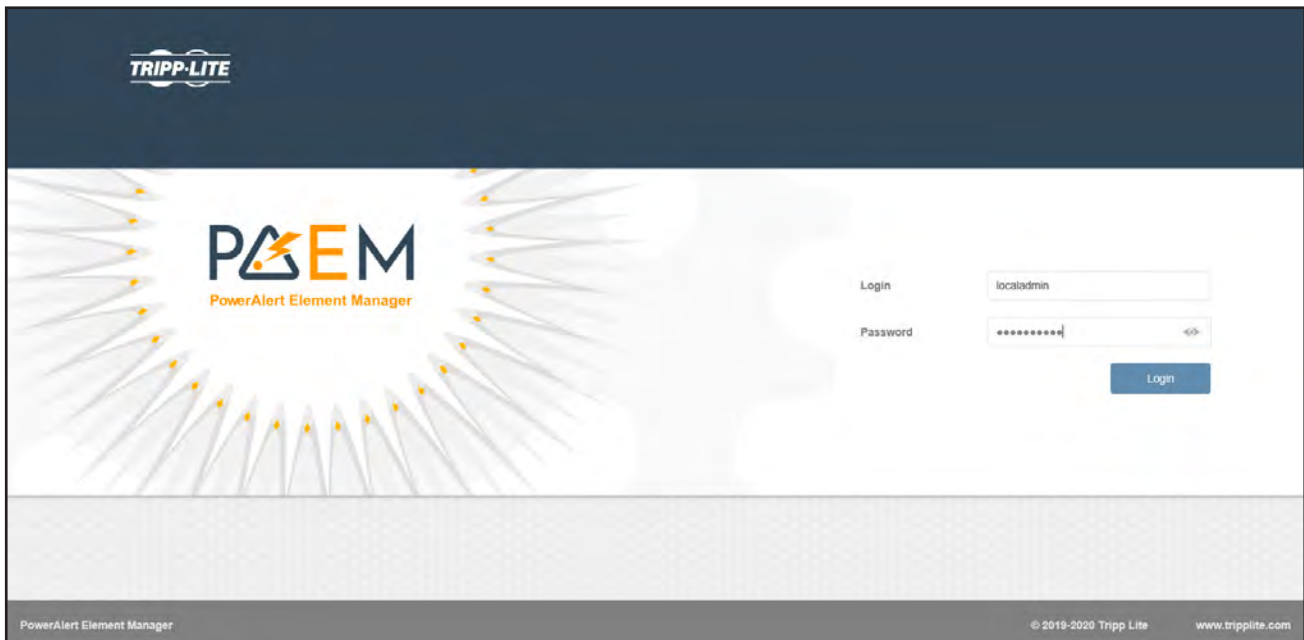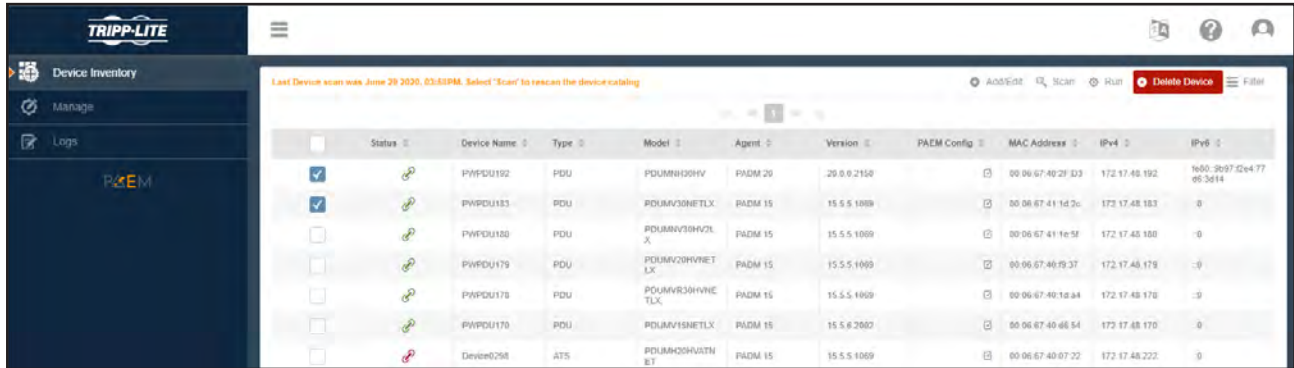
Figure 2-3: Login Page

2. Launching PAEM

Upon successful log in, PAEM displays the Device Inventory page (Figure 2-4). See section **5.1 Device Inventory** for details.

Figure 2-4: Device Inventory Page

3. PAEM Overview

3.1 PAEM Layout

The PAEM interface is comprised of three main sections (Figure 3-1):

1 **Main Menu** – Navigation to operational functions.

2 **Top Menu** – Administrative functions.

3 **Content** – Information reflective of selections made in the Main Menu or Top Menu.
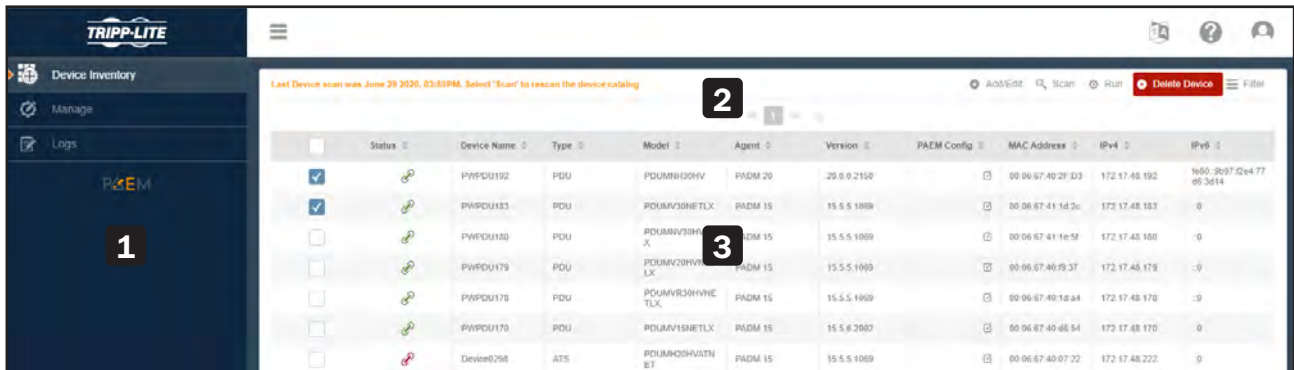
Figure 3-1: PAEM Main Sections

3.2 Navigation Elements

A number of graphical elements are used for navigation throughout the interface.

3.2.1 Tabs

Tabs are used to organize information of a common topic into logical groupings (Figure 3-2). Select a tab to view its content.
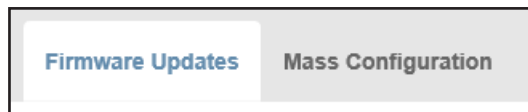
Figure 3-2: Tabs

3.2.2 Pages

Sequenced numbers with arrows indicate that the content exceeds one page (Figure 3-3). Select each to navigate pages as follows:

◄| - Go to the first pages of the content.

◄ - Go to the previous page.

number - Go directly to the selected page.

► - Go to the next page.

►| - Go to the last page of the content.

Figure 3-3.: Pages

3. PAEM Overview

3.2.3 Scroll Bars

In cases where content exceeds the size of the window, vertical and/or horizontal scroll bars appear (Figure 3-4).
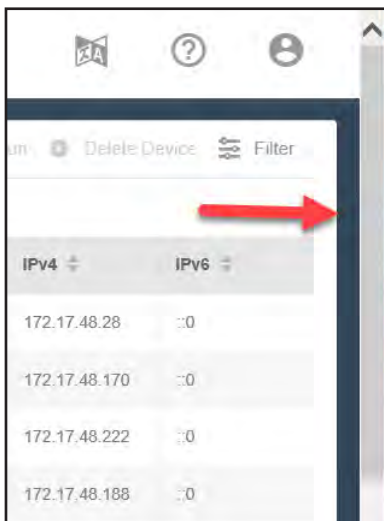
Figure 3-4: Scroll Bars

3.2.4 Back Function

Click on Back to return to the previous page (Figure 3-5).

Figure 3-5: Back Function

3.3 Adjusting Views

3.3.1 Sorting

When content is displayed in table format, the information can be sorted in the following ways (Figure 3-6):

• **Columns** – Click a column title to sort the table by that category, in ascending order.

• **Arrows** - Click the up and down arrows adjacent to the column title to sort the table in ascending or descending order, respectively.

Figure 3-6: Columns and Arrows

3. PAEM Overview

3.3.2 Filters

Click **Filter** to open a dialog box in which a variety of filtering options can be selected. Click the **Apply Filters** button to update the displayed information. Click the **Clear Filters** button to restore the default view (Figure 3-7).
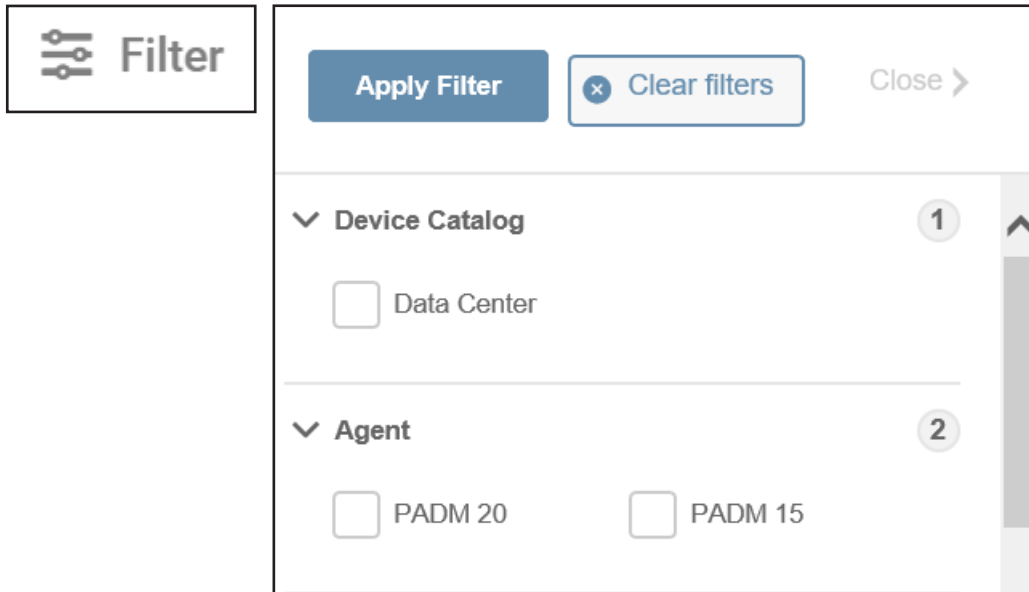
Figure 3-7: Filter Functions

3.3.3 Refresh

Click **Refresh** to update the displayed content (Figure 3-8).
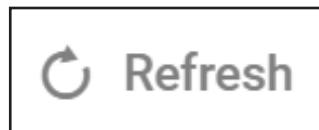
Figure 3-8: Refresh

3.3.4 Pencil

The pencil icon indicates that the item can be edited (Figure 3-9). Click the icon to open a window in which the edits can be made.

Figure 3-9: Edit

3.3.5 Export

Click **Export** to configure and generate an export of the contents (Figure 3-10).
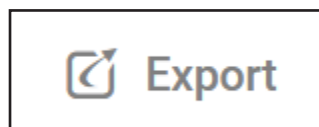
Figure 3-10: Export

3. PAEM Overview

3.3.6 Import

Click **Import** to upload source content. (Figure 3-11)

Figure 3-11: Import

3.3.7 Check for Updates

Click this link to check the Tripp Lite website for the latest firmware version(s) (Figure 3-12).

Figure 3-12: Check for Updates

3.4 Icons

3.4.1 Magnifying Glass

The magnifying glass icon indicates that the item has details (Figure 3-13). Click the icon to view the details.

Figure 3-13: Magnifying Glass

3.4.2 Delete

The ⊗ icon indicates the item can be deleted (Figure 3-14). Click the icon to mark the item for deletion; the action will change the icon color to red. To complete the deletion, click the **Delete** button (also in red).

Figure 3-14: Delete Icon

3.4.3 Checkmark

Used in the in Logs page, a green checkmark indicates no errors were encountered (Figure 3-15).

Figure 3-15: Checkmark

3. PAEM Overview

3.4.4 Warning

The Warning icon denotes that an error occurred during a process (Figure 3-16).
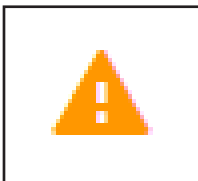
Figure 3-16: Warning Icon

3.4.5 Link

The Link icon is a hyperlink to the PowerAlert Device Manager interface of each device; click on the link to open the interface in a new web page. The icon color denotes the outcome of the most recent operation involving the device (Figure 3-17). For example, if a device encountered an error during a Mass Configuration operation, the link icon will appear yellow. If a subsequent Scan of that device is completed successfully, the icon will turn green.

• **Green** – The operation completed successfully.

• **Yellow** – An error occurred during an operation; see the Log for details.

• **Red** – The devices is offline/cannot be found.

• **Green with Yellow Lock** – The device can communicate but has not been authenticated (requires password update).
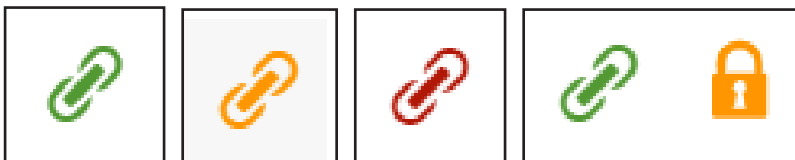
Figure 3-17: Link Icons

4. Top Menu

4.1 Language

Click the Language icon to select a personal preference for the desired language (Figure 4-1).
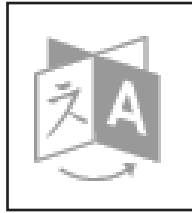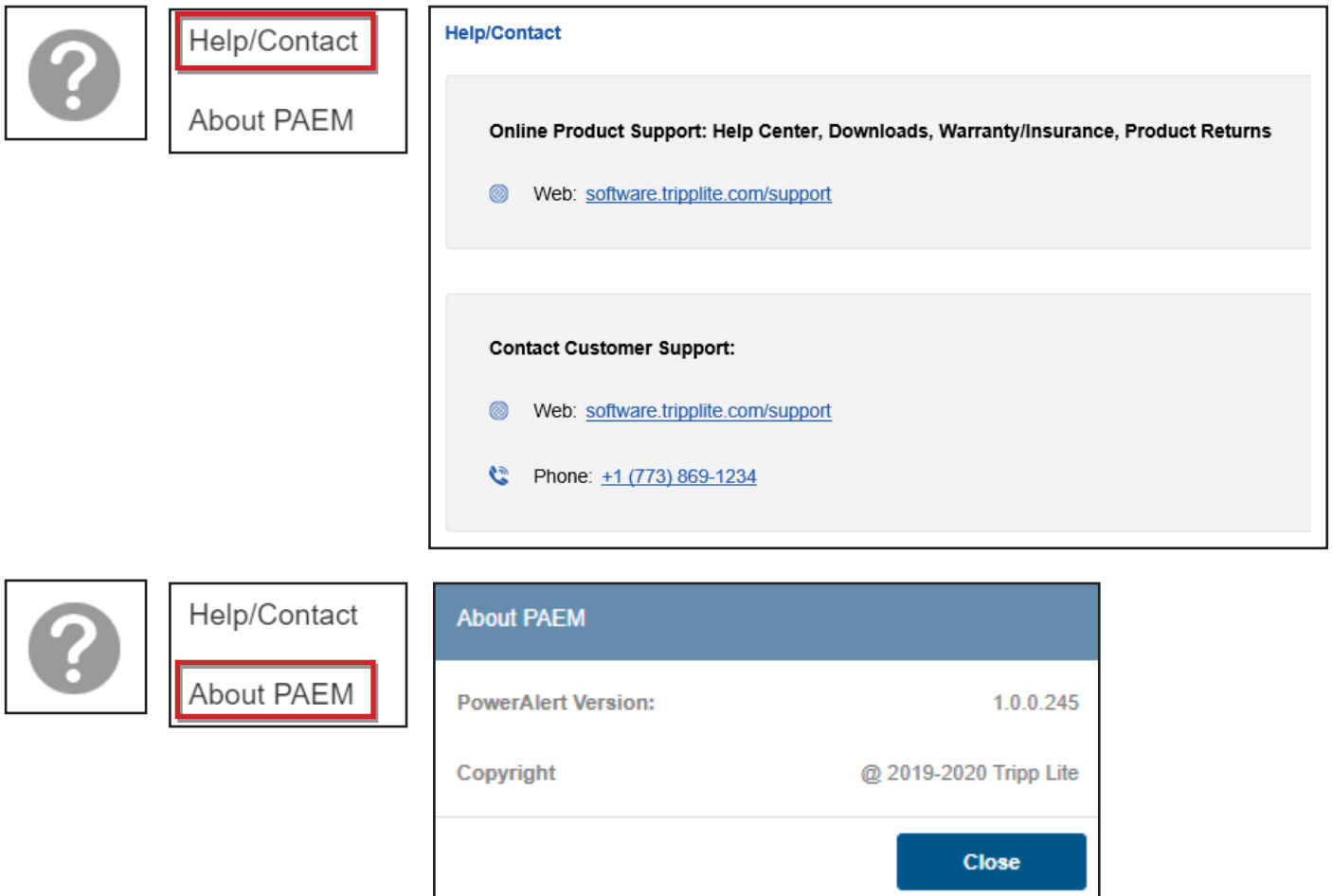
Figure 4-1: Language Icon

4.2 Support

Click the Question icon to display a sub-menu of Support items. Click **Help/Contact** to display information and links to product and technical support. Click **About PAEM** to display information about the PowerAlert Element Manager application (Figure 4-2).

Figure 4-2: Help and About PAEM

4. Top Menu

4.3 User

Click the Person icon to display a submenu of options related to the login. Click **Change Login** to change the existing password of the logged-in user. Click on the eye icon to view the plaintext password entered. Passwords must contain between 4 and 32 characters. Click **Log Out** to terminate the current session (Figure 4-3).

Figure 4-3: User Menu, Change Password and Logout

5. Main Menu

The Main Menu enables navigation to the primary functions of PAEM. Each of the Main Menu items (shown in Figure 5-1) is described in the following sections.
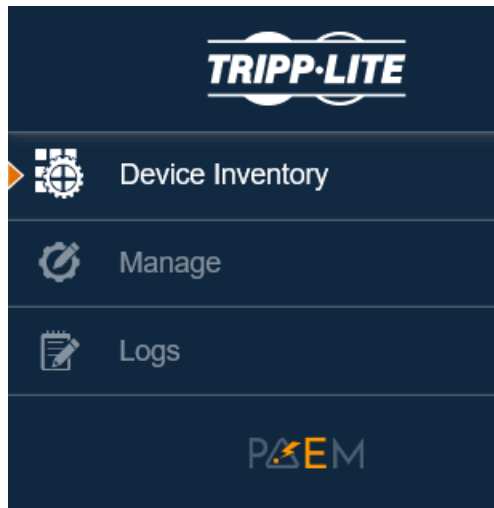
Figure 5-1: Main Menu

5.1 Device Inventory

The **Device Inventory** menu item displays a chart of all discovered devices. (Figure 5-2). On initial login, the chart will not be populated. Prior to running a scan, one or more Scan Profiles must be created.

Figure 5-2: Device Inventory

5. Main Menu

5.1.1 Creating a Scan Profile

To create a Scan Profile, click **Add/Edit** at the top of the Device Inventory page. In the Scan Profiles window that opens, click the **Add** button (Figure 5-3).
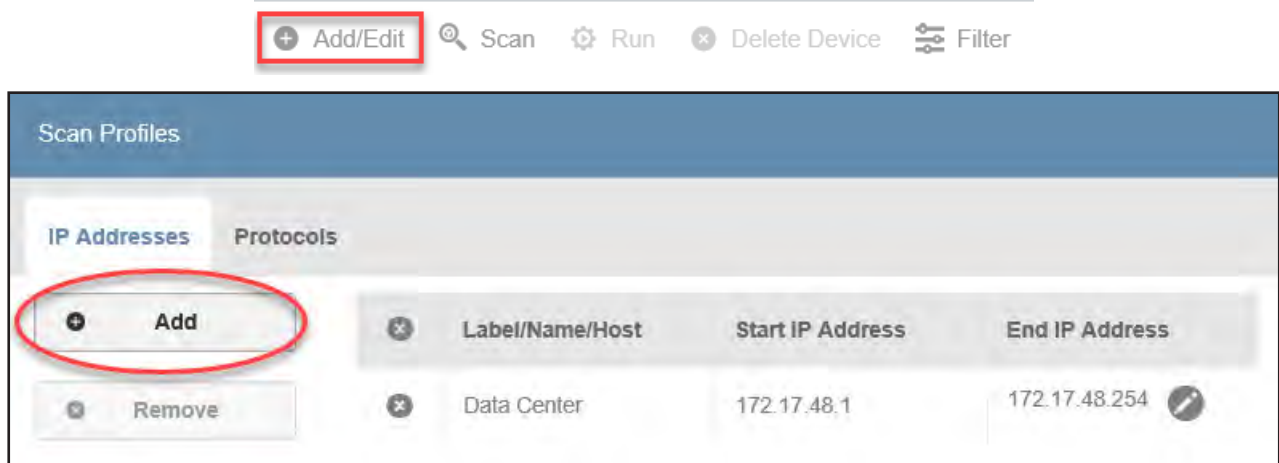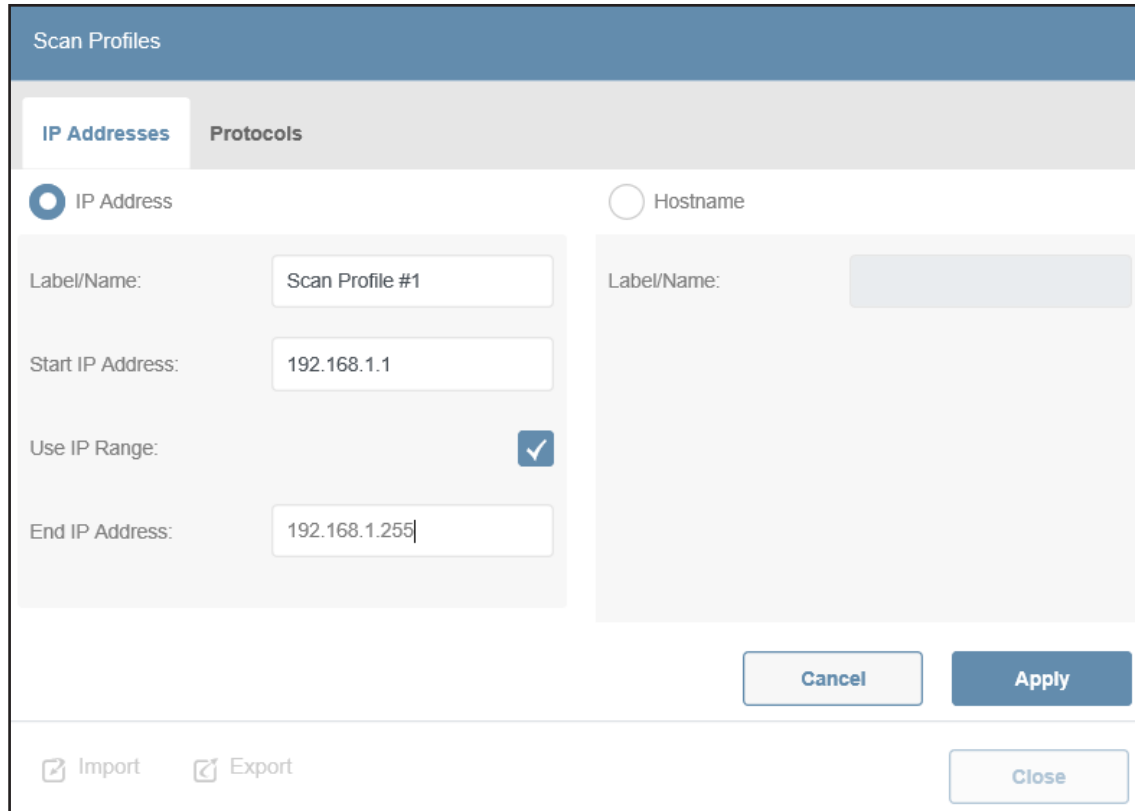

Figure 5-3: Adding a Scan Profile

A window opens to the *IP Addresses* tab, with the "IP Address" option selected by default (Figure 5-4). Enter a name for the profile as well as the starting IP address. To create a range of IP addresses, select the "Use IP Range" option and enter the ending IP address of the range. If no range is specified, only the Start IP Address will be scanned. To add a device to the profile using its hostname, select the **Hostname** option, then enter the host name in the field provided. Click the **Apply** button once all inputs have been made.

Figure 5-4: Enter IP Address Range

5. Main Menu

Next, click on the *Protocols* tab to enter all required device credentials. These credentials allow access to the device for retrieving data and executing PAEM operations. Note that multiple credentials may be required to support all functions. The table below identifies the protocols required for the each PAEM operation, for both 15.5.x and 20.x.x firmware versions. In all cases, the entered Protocol information must exactly match the credentials and authentication parameters of the device.

FUNCTION	DETAILS	15.5.x	20.x.x
Scan	For HTTP with 20.x.x, select the "Use SSL" checkbox to use HTTPS as the connection method.	SSH or SNMP	HTTP or SNMP
Mass Update	Select the "Use SSL" checkbox to use HTTPS as the connection method.	HTTP	HTTP
Mass Configuration	For 20.x.x, select the "Use SSL" checkbox to use HTTPS as the connection method.	SSH	HTTP

HTTP

- **Authentication** - Select "PADM20" for target devices running 20.x.x firmware or "PADM15" for target devices running 15.5.x firmware
- **User Name** - Input a valid administrative username
- **Password** - Input a valid administrative password
- **Port** - Input the HTTP(S) port for the target devices
- **Use SSL** - If unchecked, PAEM will use HTTP. If checked, PAEM will use HTTPS. Note that HTTP to HTTPS redirect is enabled in 20.x.x by default

SNMPv1/v2c

- **Port** - Input the SNMP port (default 161) for the target devices.
- **Community** - Input a valid SNMP community string (username) for the target devices.

Notes:

1. *SNMPv1 community of 'public' and SNMPv2c community of 'tripplite' are the default credentials for 15.5.x. These are also the respective default credentials used by PAEM. As a result, when using default credentials, no changes to either are required for PAEM to Scan 15.x.x devices via SNMP.*

2. *For firmware version 15.5.7 and above, SNMPv1 and SNMPv2c are disabled by default. These services must be first enabled on the devices for PAEM to Scan them via SNMPv1 or SNMPv2c. Alternatively, in PAEM, add an SSH protocol with administrative credentials for 15.x.x or HTTP(S) for 20.x.x.*

SNMPv3

- **Port** - Input the SNMP port (default 161) for the target devices.
- **Username** - Input a valid SNMPv3 for the target devices.
- **Privacy Mode** - Select noauthnopriv, authnopriv, or authpriv depending on target device configuration
- **Auth Protocol** - If authnopriv or authpriv are the privacy mode, select MD5 or SHA depending on target device configuration. *Note: currently all supported devices use SHA.*
- **Auth Passphrase** - If authnopriv or authpriv are the privacy mode, input the Auth Passphrase associated with the User Name
- **Privacy Protocol** - If authpriv is the privacy mode, select DES, AES, AES192, or AES256 as the privacy protocol. *Note: Currently all supported devices use AES.*
- **Privacy Passphrase-** - If authpriv is the privacy mode, input the Privacy Passphrase associated with the User Name

5. Main Menu

SSH (applies only for PAEM operations on devices running firmware version 15.5.x)

• **User Name** - Input a valid administrative username

• **Password** - Input a valid administrative password

• **Port** - Leave this value at 3664 unless instructed otherwise by Tripp Lite Technical Support

In summary, an SSH administrative credential and a HTTP(S) credential are required to get full PAEM functionality on devices running 15.x.x. For 20.x.x, only an HTTP(S) administrative credential is required for full PAEM functionality.

Figure 5-5: Protocols

To add a new protocol, click the **Add** button. In the window that opens, enter a name for the entry, then select the desired protocol from the *Type* pulldown menu. The remaining fields in the window will change to reflect the selected Type. Once all fields have been entered, click the **Apply** button.

Note: For firmware platform 20.x.x, if the Scan Profile has HTTP as the sole Protocol, ensure each device within the profile has "HTTP to HTTPS Redirection" disabled. Alternatively, change the protocol to HTTPS or add HTTPS to the Scan Profile to account for the redirection.
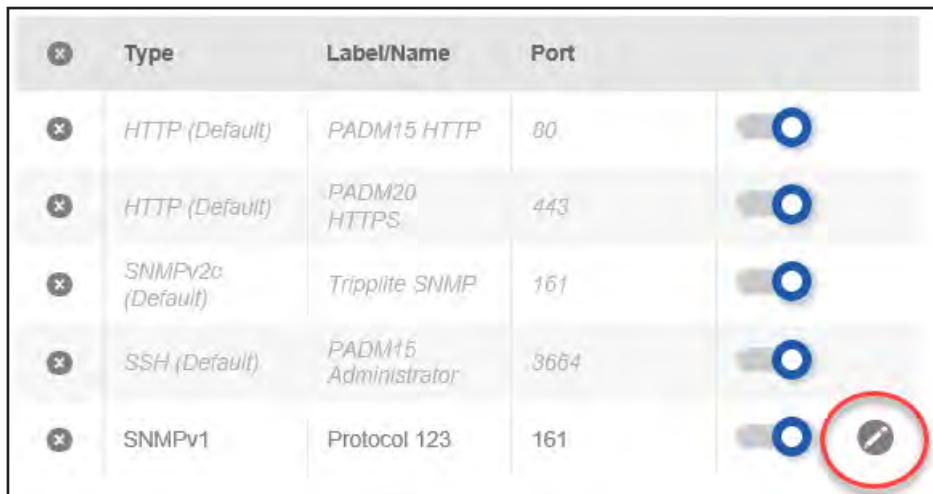
Figure 5-6: Adding a Protocol (SNMPv3 Example)

To edit a Protocol entry, click on the pencil icon to the right of the entry (Figure 5-7).
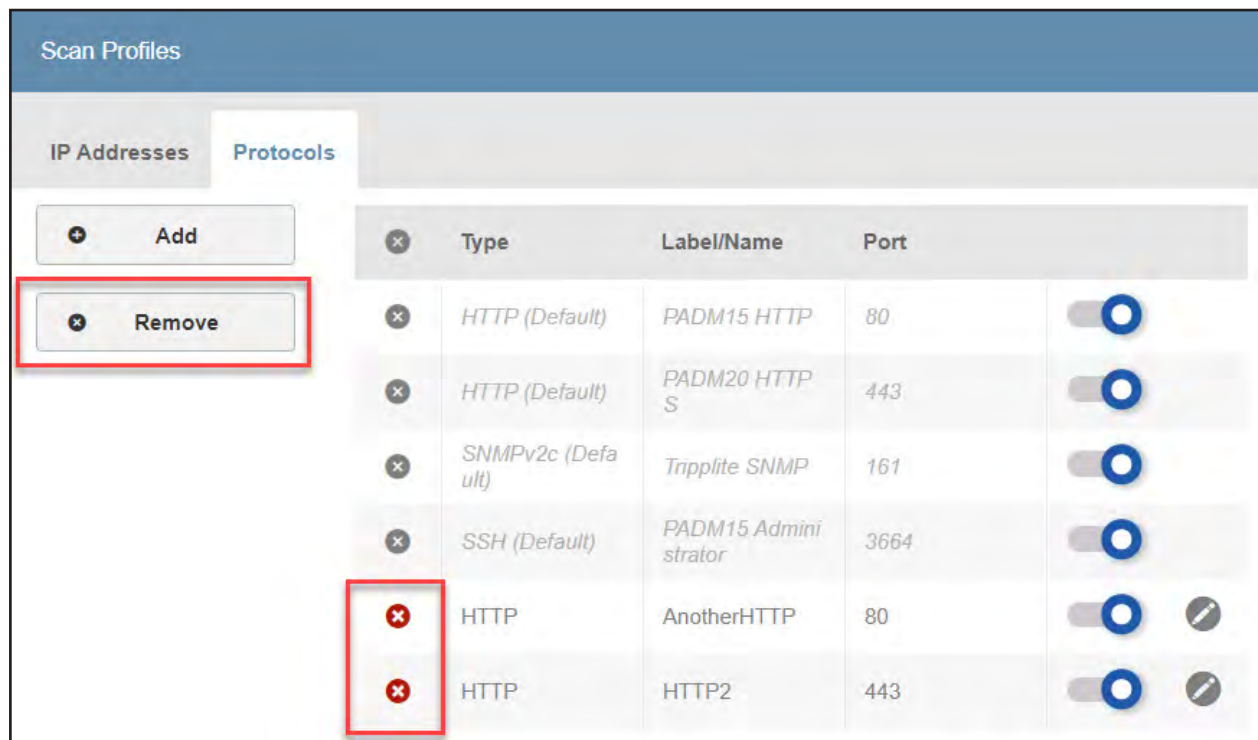
Figure 5-7: Editing a Protocol Entry

To remove one or more protocols, click the ⊗ icon of the desired protocols (which will turn red), then click the **Remove** button (Figure 5-8).

Figure 5-8: Removing Protocols

5. Main Menu

5.1.2 Importing/Exporting Scan Profiles

PAEM allows for Scan Profiles to be exported and imported. In the main Device Inventory page, click **Add/Edit** to open the Scan Profiles window; the **Import** and **Export** buttons appear at the bottom of the window (Figure 5-9).
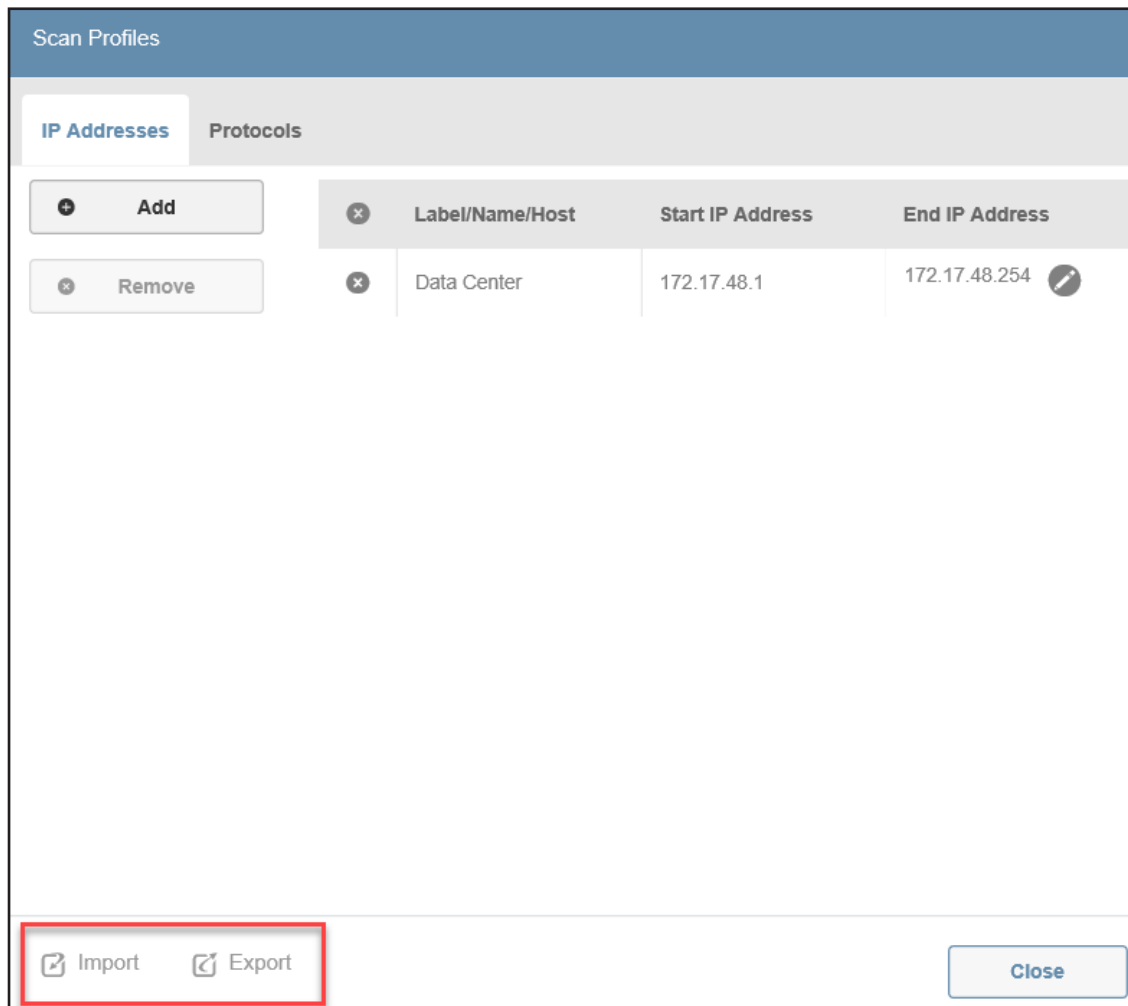
Figure 5-9: Import and Export Functions

On selecting **Import**, a standard directory tree window will open. Navigate to the location of the file, select it, then click **Open** (Figure 5-10).
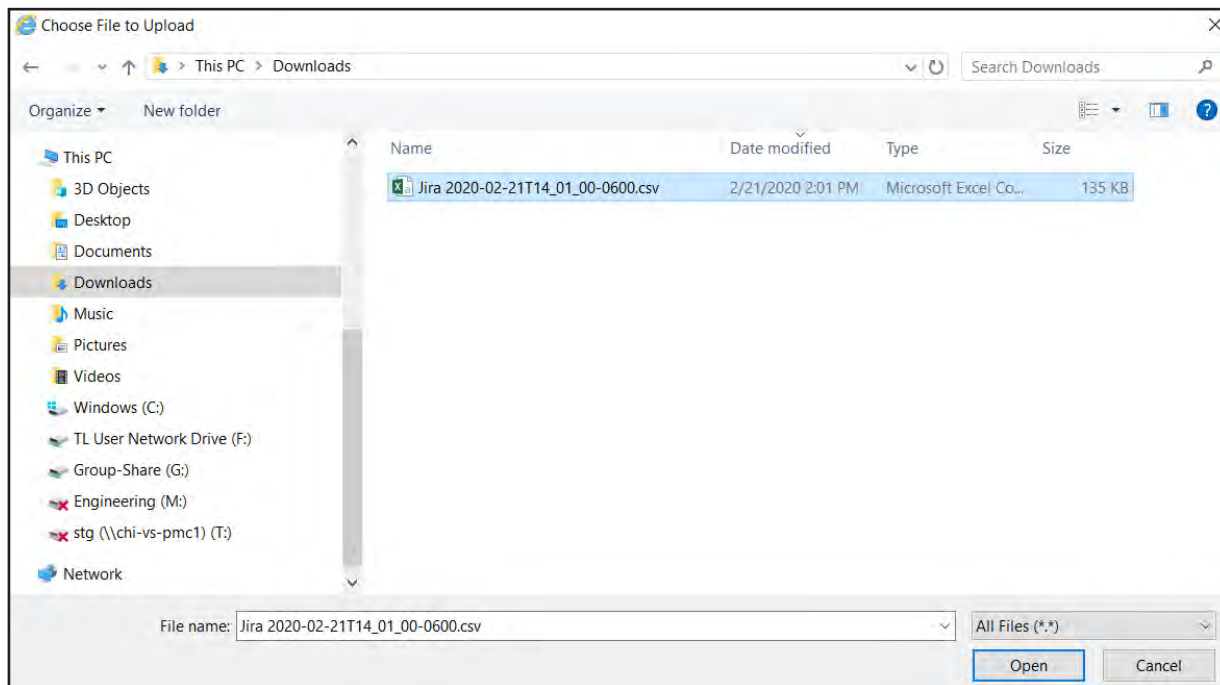
Figure 5-10: Importing a Scan Profile

To export a Scan Profile, click **Export** and select one of the file formats: CSV or XML. Upon making the selection, the export will be executed and a status message will briefly appear. The file will be stored in the Downloads folder of the computer on which PAEM is installed (Figure 5-11).
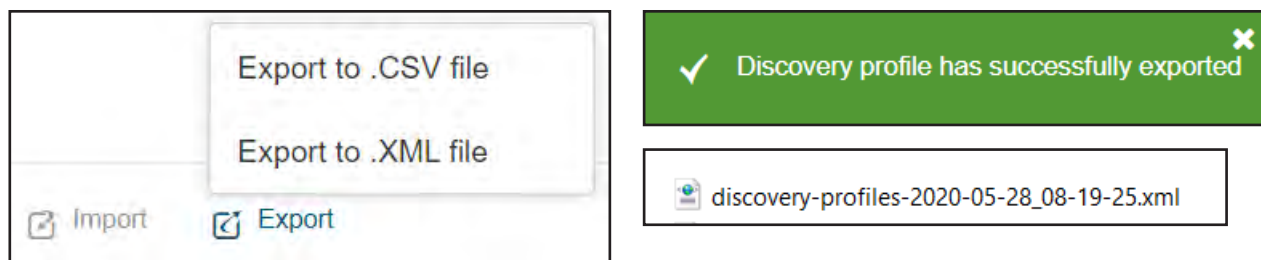
Figure 5-11: Exporting a Discovery Profile

5. Main Menu

5.1.3 Edit Scan Profiles

To edit a Scan Profile, click the pencil icon to the right of the entry. The corresponding Scan Profile window will open. When all edits have been completed, click the **Apply** button that appears in the *IP Addresses* tab of the edit window (Figure 5-12).
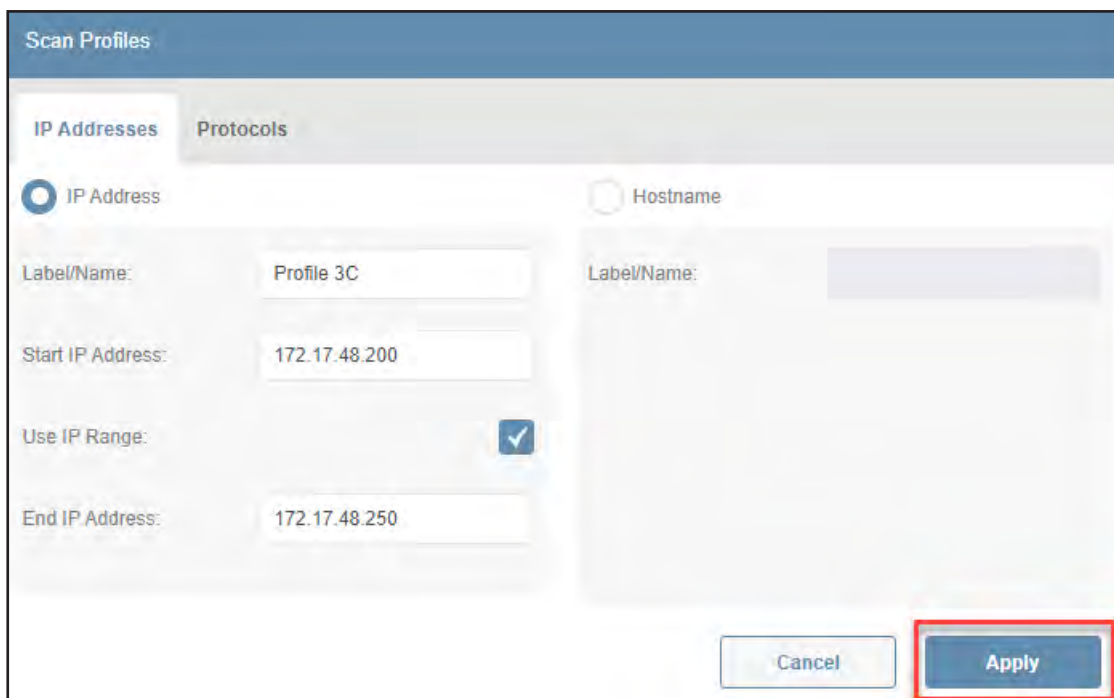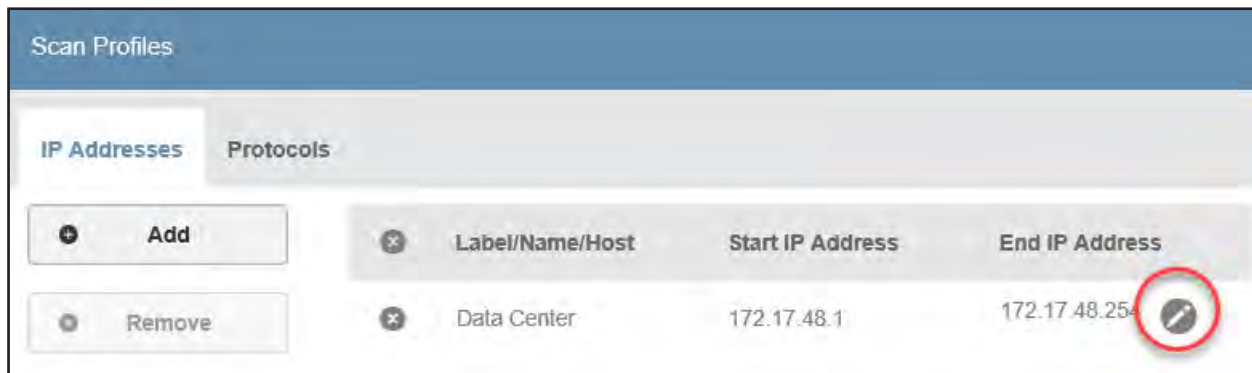
Figure 5-12: Editing a Scan Profile

5. Main Menu

5.1.4 Run Scan Profiles

In the main Device Inventory page, click **Scan**, followed by the confirmation **Scan** button. An "Active Process" icon will appear at right with a numeral indicating the number of Scan Profiles being scanned (Figure 5-13).

Figure 5-13: Scanning Discovery Profiles

Click on the "Active Process" icon to expand it and display details about the scan. The number represents the quantity of profiles being scanned. Click the **Cancel** button to terminate the scan. Click on the icon again to shrink the window (Figure 5-14).

Figure 5-14: Active Processes

When the process has completed, the Device Inventory chart will populate with all discovered devices (Figure 5-15).

Figure 5-15: Device Inventory Chart

5. Main Menu

5.1.5 Device Inventory Overview

	Status ⬍	Device Name ⬍	Type ⬍	Model ⬍	Agent ⬍	Version ⬍	PAEM Config ⬍	MAC Address ⬍	IPv4 ⬍	IPv6 ⬍
☐	🔗	SRCOOL12K131	AC	SR(X)COOL	PADM 15	15.5.6.2002	☑	00:06:67:41:f7:34	172.17.48.131	::0
☐	🔗	PWPDU192	PDU	PDUMNH30HV	PADM 15	15.5.5.1069	☑	00:06:67:40:2f:d3	172.17.48.192	::0
☐	🔗	PWPDU183	PDU	PDUMV30NETLX	PADM 15	15.5.5.1069	☑	00:06:67:41:1d:2c	172.17.48.183	::0

Figure 5-16: Device Inventory Content

Referring to Figure 5-16 above, the Device Inventory chart is comprised of the following columns (left to right):

- **Checkbox** – Allows selection of one or more devices to undergo PAEM operations. To select all devices, check the box in the column header.
- **Status** – A colored icon denotes the device status; refer to section **3.4.5 Link** for descriptions of the icons and colors.
- **Device Name** – The default name or user-customized name of the device.
- **Type** – The type of device (i.e. UPS, PDU, ATS, AC).
- **Model** – The model number of the device.
- **Agent** – The name of the LX Platform agent.
- **Version** – The version of the agent (e.g. the firmware version of the LX card).
- **PAEM Config** – Click the icon in this column to download the device's configuration for use in mass configuration operations.
- **MAC Address** – The MAC address of the device
- **IPv4** – The IPv4 address of the device
- **IPv6** – The IPv6 address of the device

5.1.6 Deleting a Device

To remove a device from the Device Inventory, select its check box and then click **Delete Device** followed by the **Delete** button in the confirmation window (Figure 5-17).

Note: Deleting a device does not remove it from a Scan Profile. The device may re-appear in the Device Inventory during the next scan.

Figure 5-17: Deleting a Device

5. Main Menu

5.1.7 Configuring Device(s)

There are two ways to import device configurations for use as source files for mass configuration operations:

1. Click the icon in the **PAEM Config** column of the Device Inventory table for the source device (Figure 5-18).

	Status ⇕	Device Name ⇕	Type ⇕	Model ⇕	Agent ⇕	Version ⇕	PAEM Config ⇕	MAC Address ⇕
☐	🔗	Device0011	PDU	PDU3EVSR6L2130	PADM 20	20.0.0.1892	☑	
☐	🔗	DCPDU29	PDU	PDUMVR30HVNETLX	PADM 15	15.5.6.2002	☑	
☐	🔗	Device4378	UPS	SU5000RT4UHV	PADM 20	20.0.0.1878	☑	
☐	🔗	DCUPS78	UPS	SUINT3000RTXL2U	PADM 15	15.5.5.1069	☑	
☐	🔗				PADM 15	15.5.5.1069	☑	
☐	🔗	Device0017	PDU	PDUMNH30	PADM 15	15.5.5.1069 Import configuration	☑	
☐	🔗	Device2519	UPS	SU10000RT3UPM	PADM 20	20.0.0.1892	☑	

Figure 5-18: Import Configuration from Device Inventory Table

On clicking the icon, an "Active Process" icon will appear in the upper right column as well as a status message regarding the import (Figure 5-19).
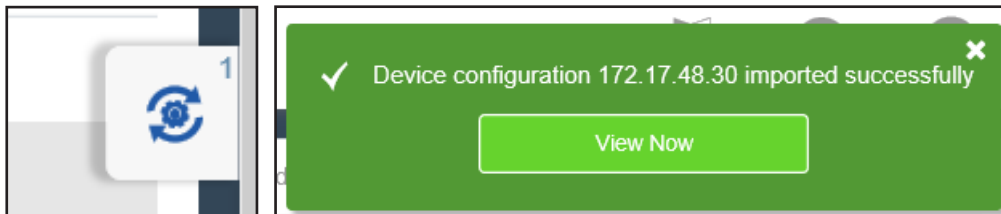
Figure 5-19: Import Progress and Status Message

2. In the *Mass Configuration* tab of the **Manage** menu item, click **Import** (Figure 5-20). In the standard directory tree that opens, navigate to the location of the file, select it and click **Open**.
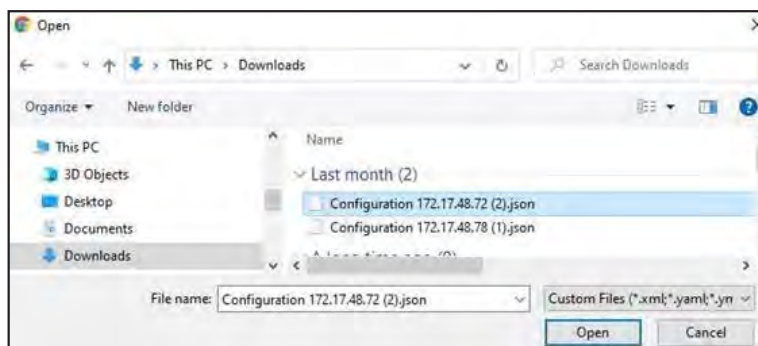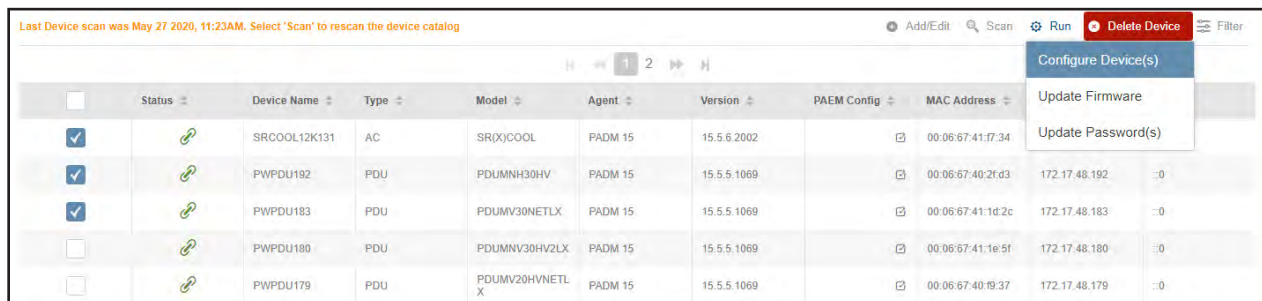
Figure 5-20: Mass Configuration Tab/Import

5. Main Menu

To configure one or more devices, select their checkboxes in the Device Inventory chart. Next, click **Run** and select the **Configure Device(s)** option (Figure 5-21).

Figure 5-21: Configure Device(s) Option

In the "Select Configuration File" window that opens, select the desired configuration file, then click the **Select** button (Figure 5-22). If the required configuration file does not appear in the list, click on the Open icon in the upper right corner to browse for and select a different configuration file.
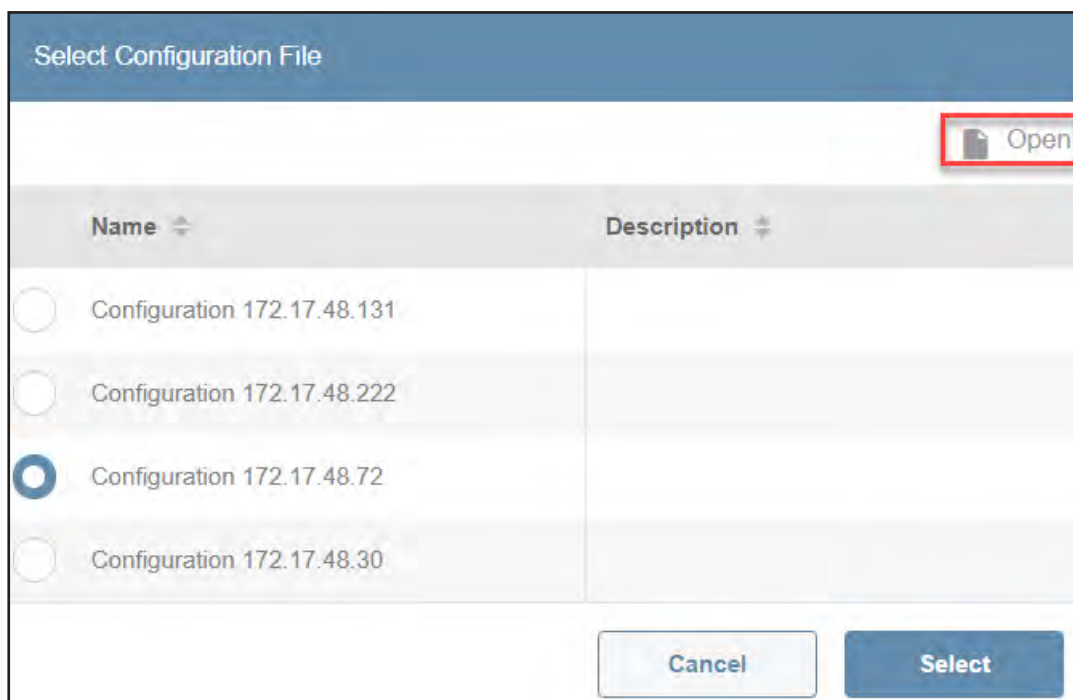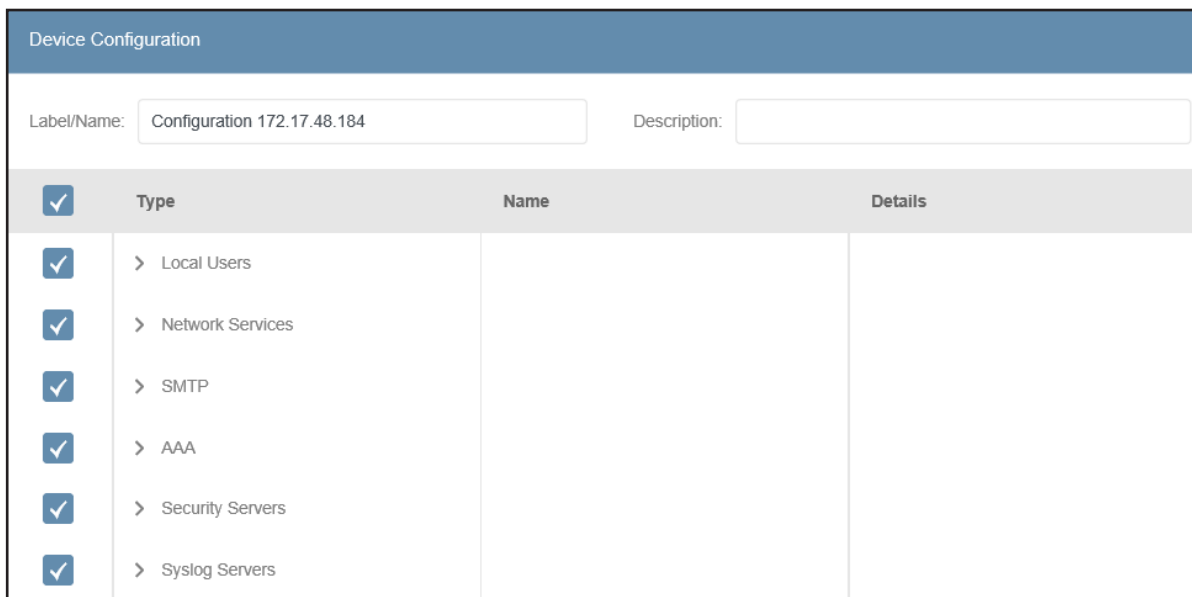
Figure 5-22: Select a Configuration File

A window will open displaying the contents of the device configuration (Figure 5-23). If desired, edit the name of the configuration file in the "Label/Name" field and add information about the configuration in the "Description" field.

Figure 5-23: Configuration File Contents

Click on the caret icon (>) next to an item to expand it, displaying its details (Figure 5-24).

Figure 5-24: Expanded Element (AAA)

5. Main Menu

Using the checkboxes, select all items that are to be included in the mass configuration. If desired, click Export at the bottom of the window; this will export the current configuration to the Downloads folder of the computer. Click the **Next** button at the bottom of the window once all selections have been made (Figure 5-25).

Figure 5-25: Selected Configuration Elements

5. Main Menu

A window will appear in which access credentials can be entered. During a Mass Configuration, passwords and related authorization parameters are not retrieved from the source configuration. To include these passwords and parameters in the mass configuration, they must be entered in this window (Figure 5-26). Note that there are multiple tabs in which passwords/parameters are to be entered: *Local Users, SNMPv1, SNMPv2 and SNMPv3*. Once all passwords have been entered, click the **Run** button.

Note: If configuration items requiring passwords (e.g. Local Users) are selected for inclusion in the Mass Configuration, but the passwords and authorization parameters are not entered, devices will fail Mass Configuration operations.
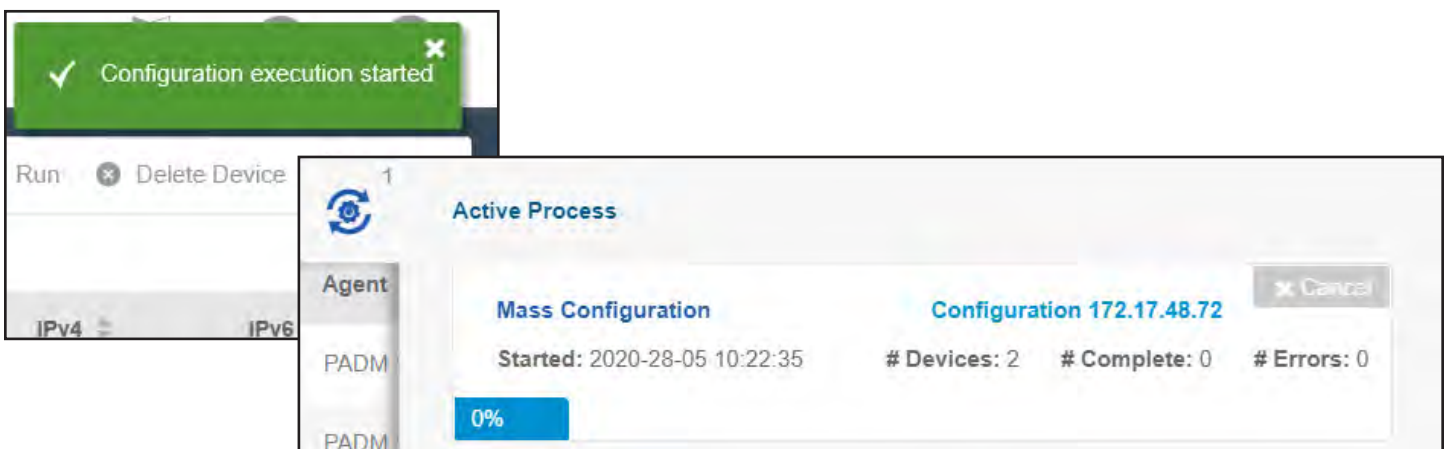

Figure 5-26: Enter Device Passwords

A progress indicator and status message will appear denoting the start of the mass configuration (Figure 5-27).

Note: the configuration process may take more than 20 minutes to complete and the progress indicator may show "0%" for a majority of that time. Please be patient.
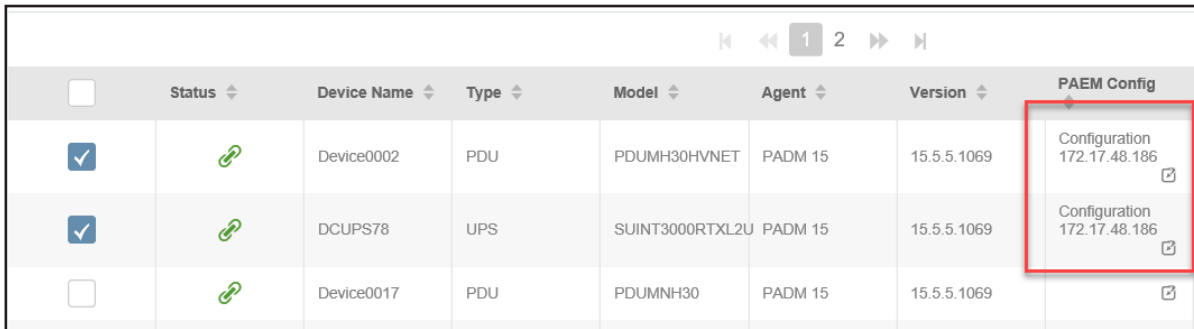

Figure 5-27: Active Process Icon and Message.

Upon completion, the "PAEM Config" column will display the updated configuration file name for the devices that underwent the mass configuration (Figure 5-28).

	Status	Device Name	Type	Model	Agent	Version	PAEM Config
☑	🔗	Device0002	PDU	PDUMH30HVNET	PADM 15	15.5.5.1069	Configuration 172.17.48.186
☑	🔗	DCUPS78	UPS	SUINT3000RTXL2U	PADM 15	15.5.5.1069	Configuration 172.17.48.186
☐	🔗	Device0017	PDU	PDUMNH30	PADM 15	15.5.5.1069	

Figure 5-28: Updated PAEM Config Column

5.1.8 Updating Firmware

To update the LX Card firmware on one or more devices, select their checkboxes in the Device Inventory table. Next, click **Run** and select the **Update Firmware** option (Figure 5-29).

Figure 5-29: Update Firmware Option

To check whether a new firmware version is available for download from the Tripp Lite website, click on **Check for Updates**. The result of the check will appear in the window (Figure 5-30).
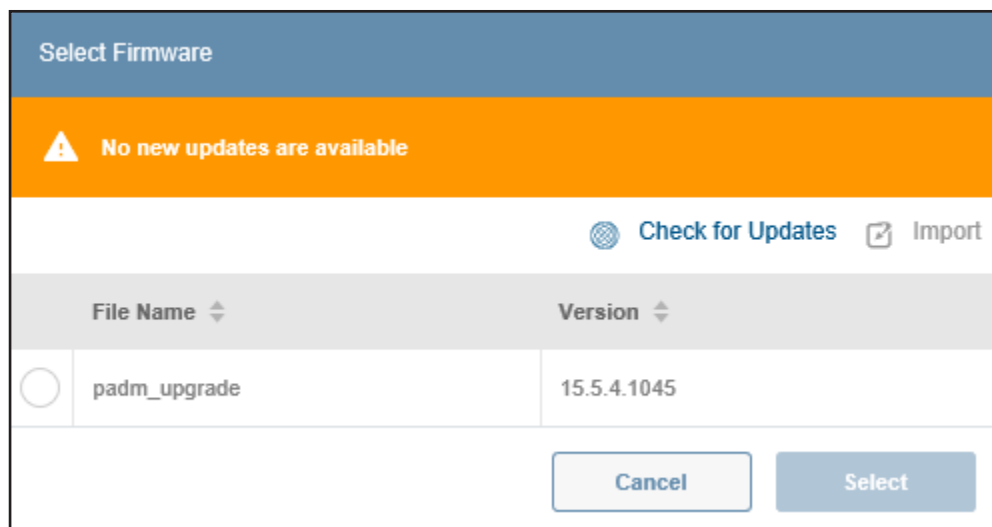

Figure 5-30: Firmware Availability Message

5. Main Menu

To upload a firmware file from a known location, click **Import**, then browse to the location. Select the file, then click **Open** (Figure 5-31).
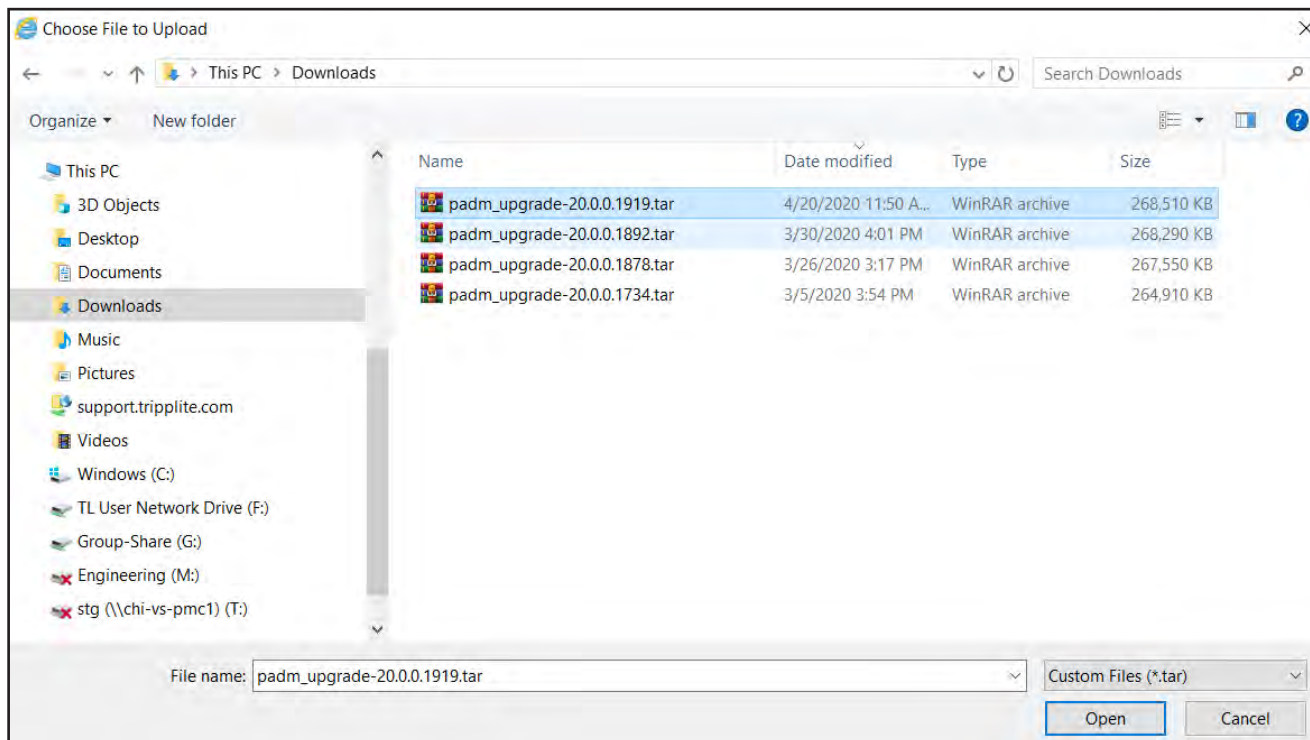

Figure 5-31: Importing an Firmware Update File

The "Select Firmware" window will update to reflect the imported file. Select the desired file, then click the **Select** button (Figure 5-32).
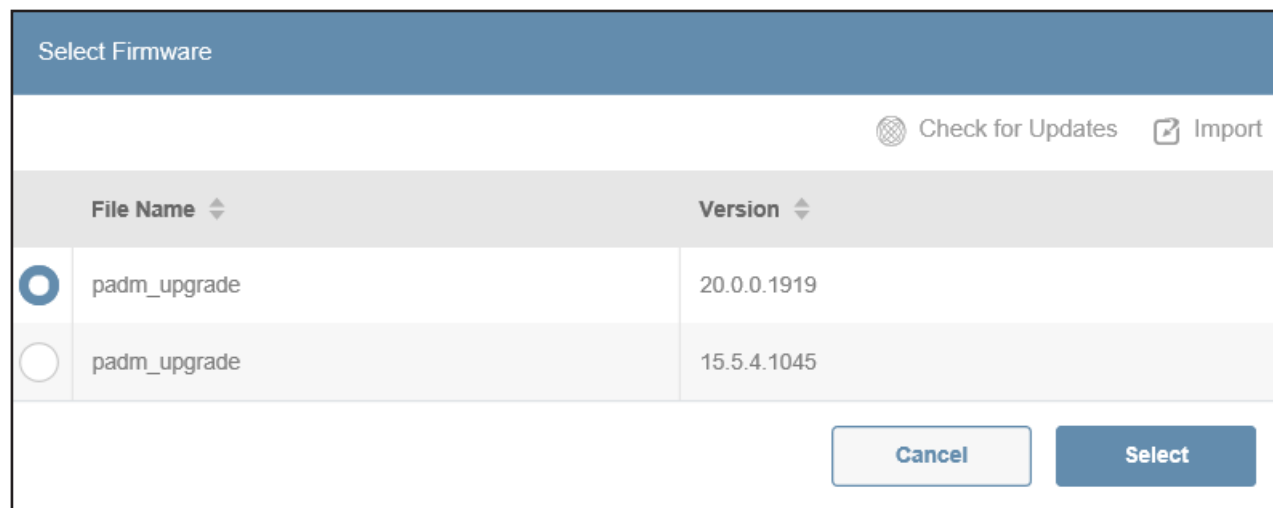

Figure 5-32: Select Firmware

5. Main Menu

The system will perform a check of the selected firmware version against the selected devices. A message reflective of the check will appear in the box. Below are examples of a standard update message and one involving a downgrade. Click the **Run** button to continue (Figure 5-33).
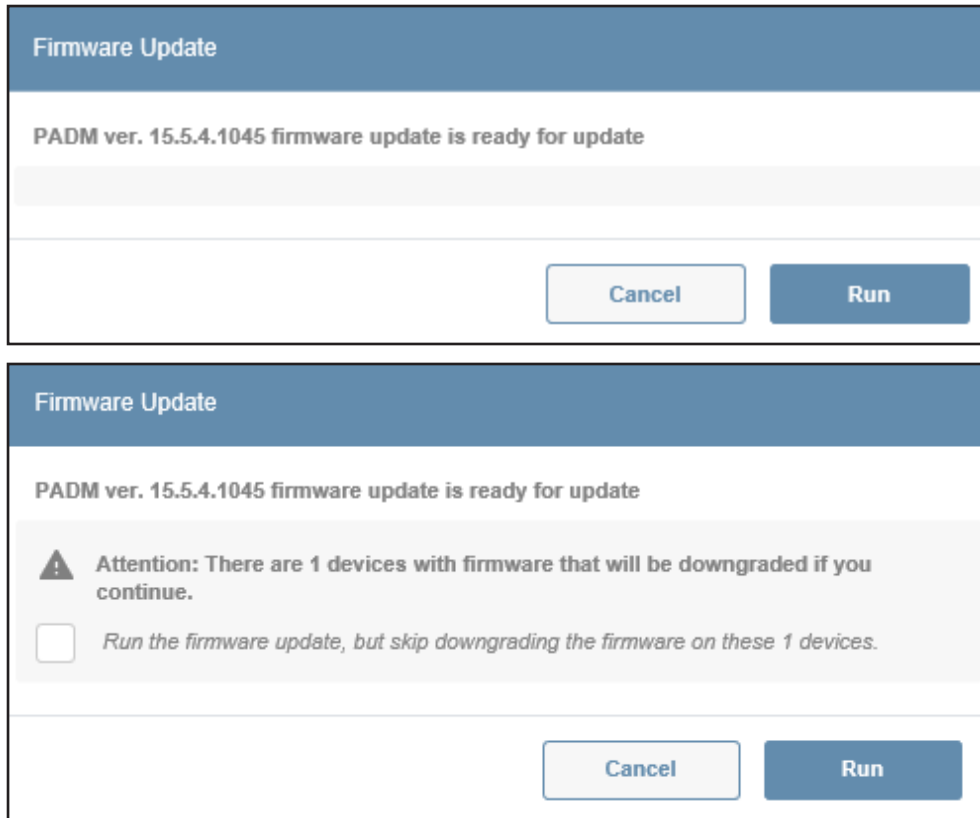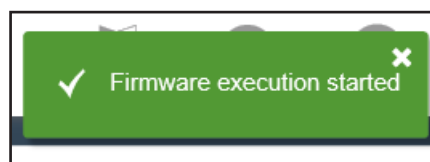

Figure 5-33: Firmware Check Messages

A status message will appear denoting the start of the firmware update. Warning icons will appear in the Status column in the Device Inventory page to reflect that the devices are undergoing the update (Figure 5-34).

Figure 5-34: Status Message and Status Column Indication

5. Main Menu

The "Active Process" icon will appear in the upper right. Click the icon to display information about the process. Press the **Cancel** button to terminate the process (Figure 5-35).

Note: The update process may take several minutes. Please be patient.
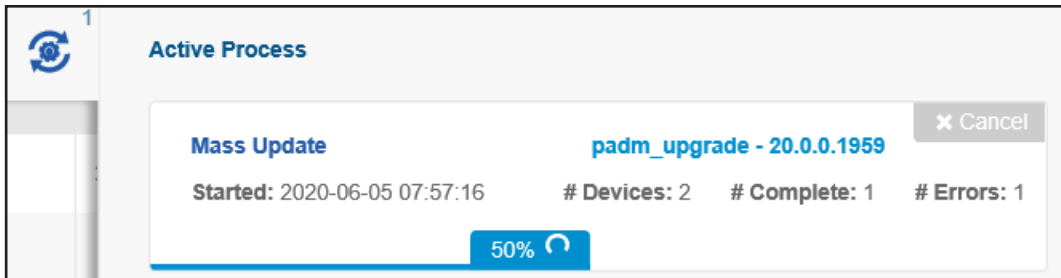

Figure 5-35: Active Process – Firmware Update

5.1.9 Update Password

Certain Regulations require that default passwords must be changed on initial use. Also, PADM20 security policies (i.e. maximum password age reached) may force changing the password. In both cases, this condition will be denoted by the yellow lock icon in the Device Inventory screen. Use the Update Password function to change the user password on the device(s). Afterwards, be sure to update the respective Scan Profile Protocol (section **5.1.1 Creating a Scan Profile**) in PAEM with the same password. Alternatively, first create a new Scan Profile Protocol entry with the new password, then execute the Change Password function to update the user password on the device(s). To update the login password one or more devices, select their checkboxes in the Device Inventory page, then click **Run** and select the **Update Password(s)** option. A window will open in which the new password can be entered (Figure 5-36).

Note: The password length must be between 4 and 32 characters.

Click the **Run** button when the new password has been entered and confirmed (Figure 5-36).
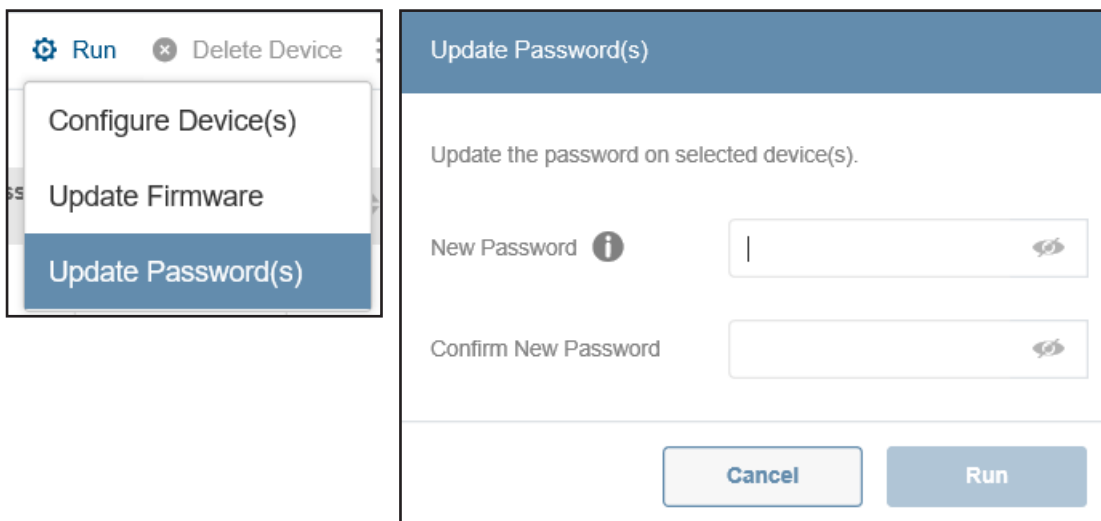

Figure 5-37: Update Passwords

A status message will appear indicating that the password change is being applied (Figure 5-38).
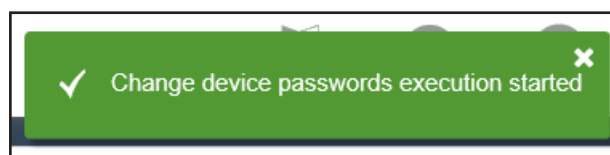

Figure 5-38: Status Message for Password Change

Note: When changing the devices' passwords, ensure all Scan Profiles are also updated with the new password(s).

5. Main Menu

5.2 Manage

The **Manage** menu item is comprised of two tabs: *Firmware Updates* and *Mass Configuration*. The *Firmware Updates* tab displays a list of firmware files that have been imported into PAEM (Figure 5-39).
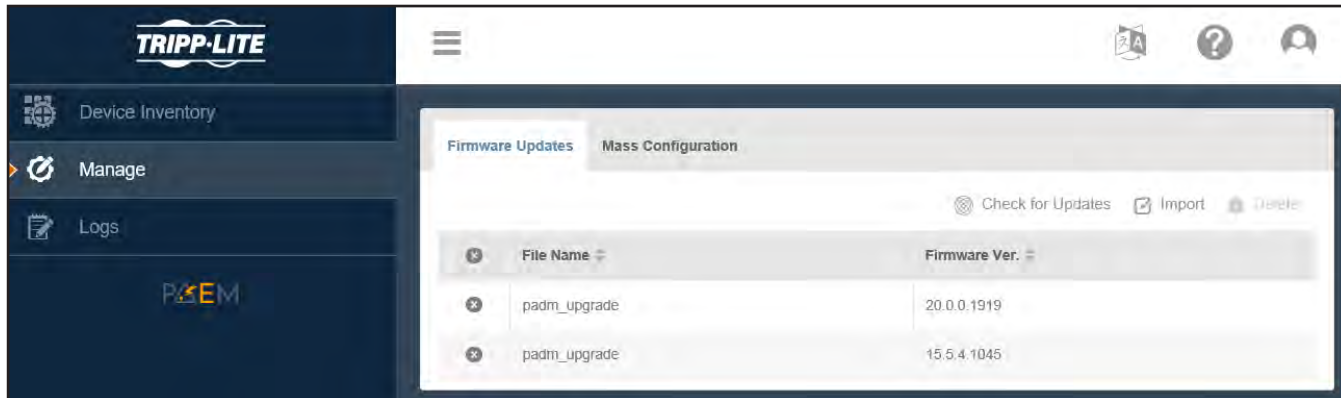

Figure 5-39: Firmware Updates Tab

Click on **Check for Updates** to confirm whether a new firmware version is available in comparison to the ones already imported. This action checks for new firmware versions of both 15.5.x and 20.x.x. A message will appear displaying the results of the search. If new firmware is available, PAEM will automatically upload it and display a dialog box from which the update can be initiated (Figure 5-40).
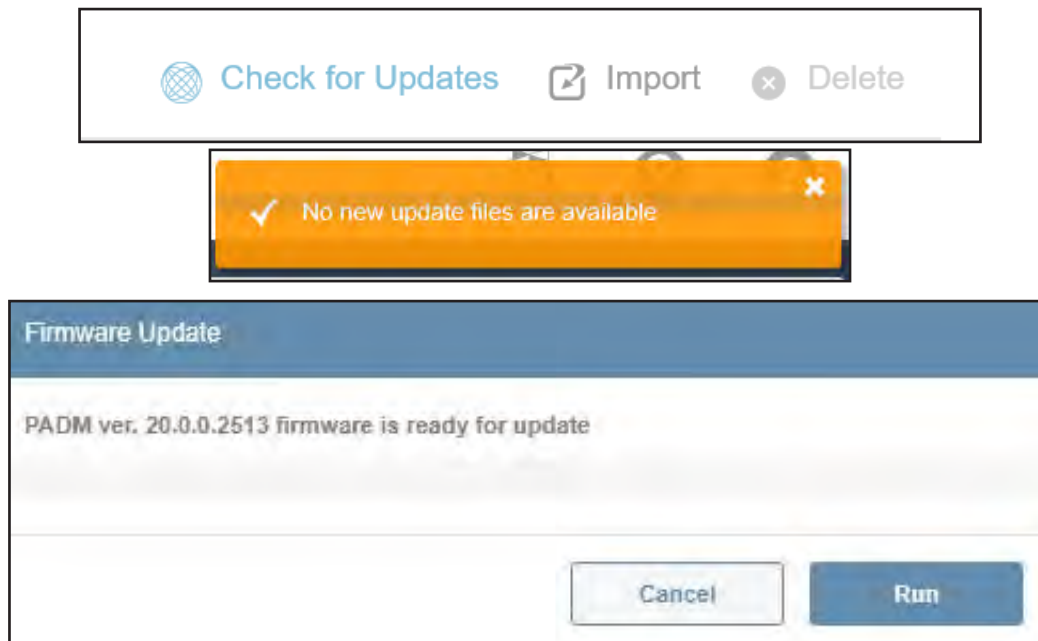
Figure 5-40: Check for Updates

Click **Import** to browse for a firmware file (Figure 5-41). This action is identical to the one described in section **5.1.7 Configuring Device(s**).

Figure 5-41: Firmware Import

To remove one or more Firmware files from the list. Click the ⊗ icon to the left of each required file, then click the **Delete** button at right. In the confirmation window that appears, click the **Delete** button.
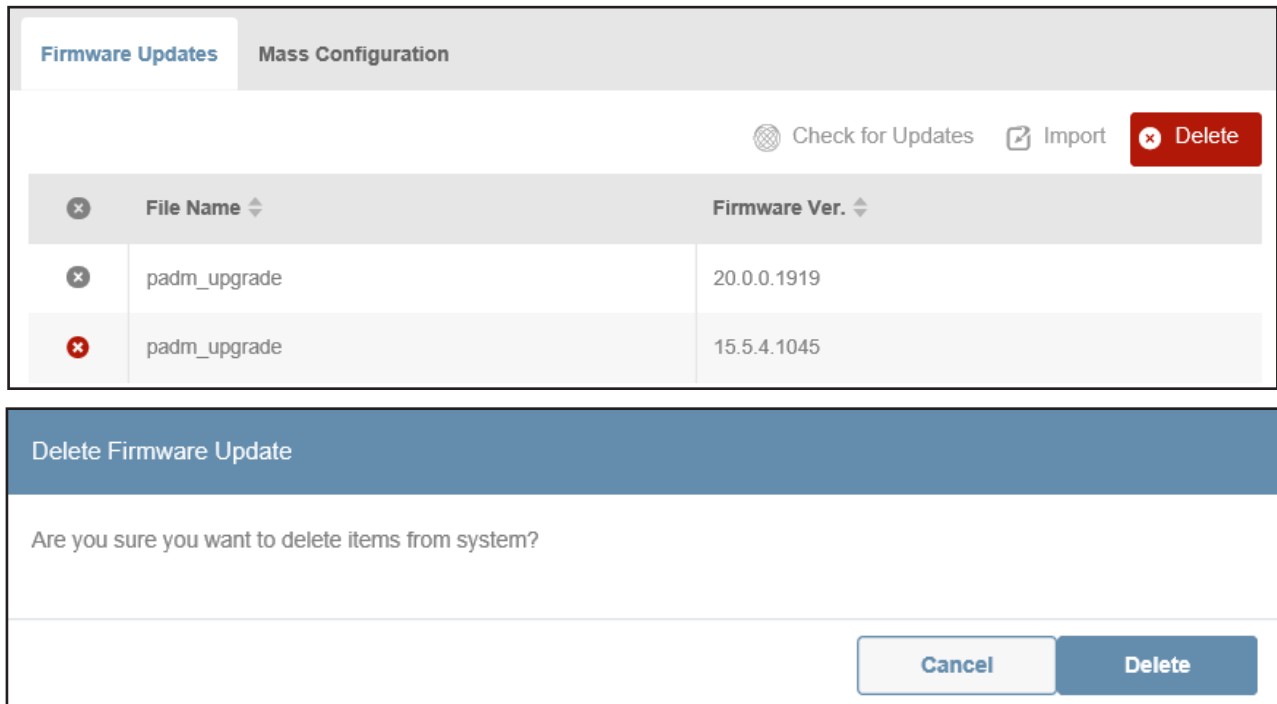

Figure 5-42: Deleting Firmware Files

The *Mass Configuration* tab displays a list of imported device configurations. Click **Import** to browse for a stored configuration file (Figure 5-43). This is identical to the Import function described in section **5.1.7 Configuring Device(s)**.
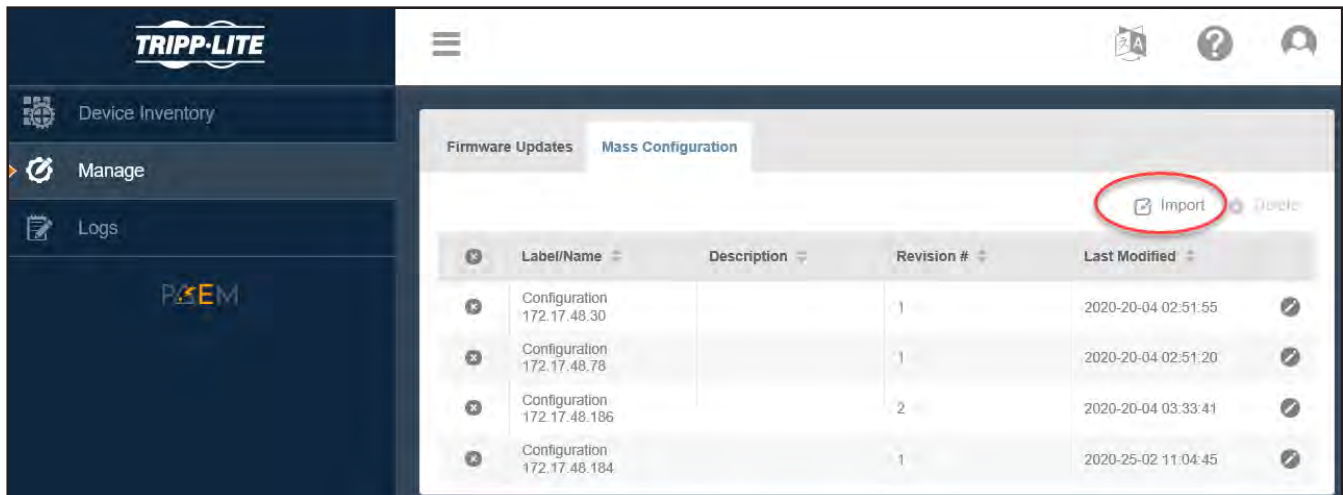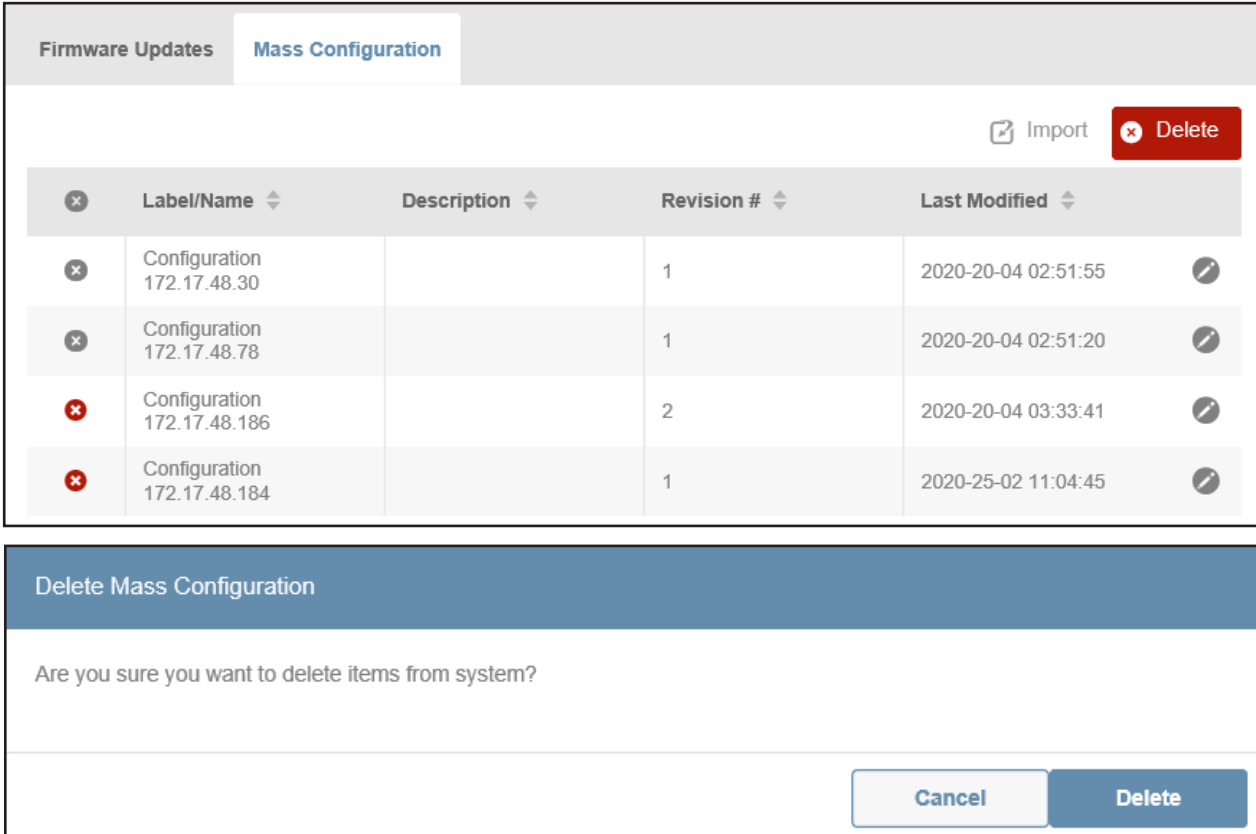
Figure 5-43: Mass Configuration Tab and Import

5. Main Menu

To remove one or more Configuration files from the list, click the ⊗ icon to the left of each required file, then click the **Delete** button at right. In the confirmation window that appears, click the **Delete** button (Figure 5-44).
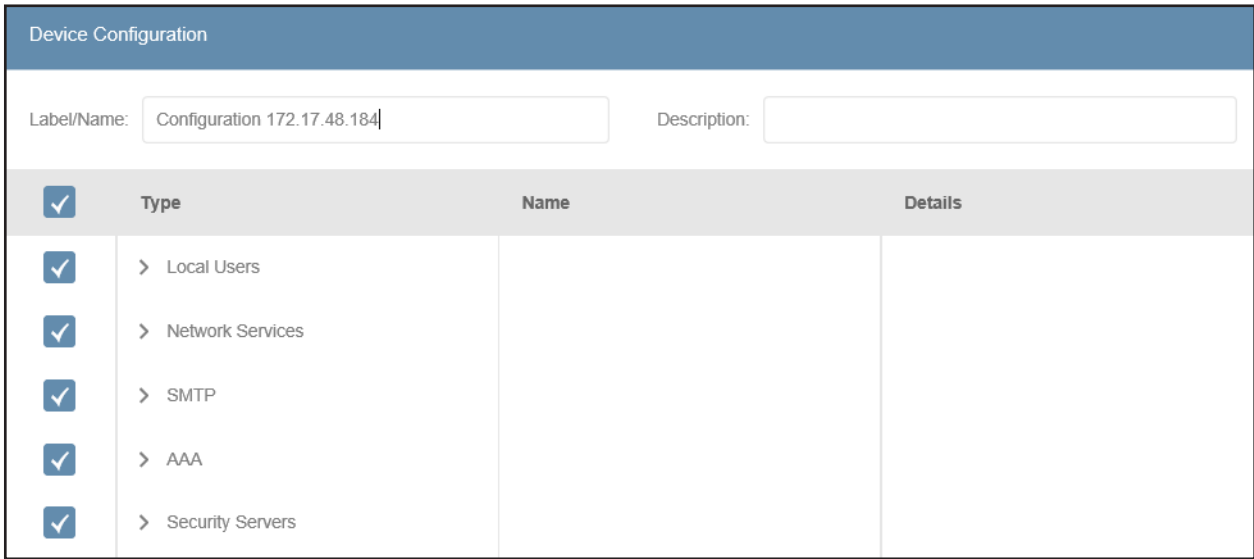

⊗	Label/Name ⇕	Description ⇕	Revision # ⇕	Last Modified ⇕	
⊗	Configuration 172.17.48.30		1	2020-20-04 02:51:55	✎
⊗	Configuration 172.17.48.78		1	2020-20-04 02:51:20	✎
⊗	Configuration 172.17.48.186		2	2020-20-04 03:33:41	✎
⊗	Configuration 172.17.48.184		1	2020-25-02 11:04:45	✎

Delete Mass Configuration

Are you sure you want to delete items from system?

Cancel | Delete

Figure 5-44: Delete Configurations

To edit a configuration, click the pencil icon to the right of the item. This opens the Device Configuration window described in section **5.1.7 Configuring Device(s)** (Figure 5-45).

Figure 5-45: Device Configuration Window

During a Mass Configuration, if PAEM encounters an issue when configuring a device, it will stop all further configuration of the device. The device will retain the changes made during the Mass Configuration to that point. PAEM will neither roll back nor proceed with configuring that device.

5. Main Menu

5.3 Logs

The **Logs** menu item displays a record of all actions taken by PAEM, as displayed in chronological order with the most recent events at the top of the list (Figure 5-46). A green checkmark indicates the process completed successfully. A yellow triangle indicates an error occurred during the process.

Figure 5-46: Logs Page

To view details of a specific event, click on the magnifying glass to the right of the item. Note that within the details window, further details may be available via the magnifying glass icon, at right. Click **Back** to return to the main Logs page (Figure 5-47).

Figure 5-47: Log Entry Details

6. Technical Support

For questions or information related to PADM, please contact Tripp Lite Tech Support:

Phone: 773.869.1234 (7am – 6pm CST).

Web: tripplite.com/support

Email: techsupport@tripplite.com

Note: Online Product Support and Tripp Lite Technical Support contact information are also available via the Help icon in the PADM Top Menu.

Tripp Lite has a policy of continuous improvement. Specifications are subject to change without notice.
Photos and illustrations may differ slightly from actual products.

TRIPP·LITE

OVER 95 YEARS
Manufacturing Excellence.

1111 W. 35th Street, Chicago, IL 60609 USA • tripplite.com/support

20-10-224 93-3B5A_RevA